

FORM PTO-1390 (Modified) (REV 11-98)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY'S DOCKET NUMBER 6761-60186	
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371				U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1.5) 097762649	
INTERNATIONAL APPLICATION NO. PCT/EP99/05879		INTERNATIONAL FILING DATE 11 August 1999		PRIORITY DATE CLAIMED 11 August 1998	
TITLE OF INVENTION SECURITY SYSTEM					
APPLICANT(S) FOR DO/EO/US NEIFER, Wolfgang					
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:					
<ol style="list-style-type: none"> <input checked="" type="checkbox"/> This is a FIRST submission of items concerning a filing under 35 U.S.C. 371. <input type="checkbox"/> This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371. <input type="checkbox"/> This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1). <input checked="" type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date. <input type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371 (c) (2)) <ol style="list-style-type: none"> <input type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau). <input type="checkbox"/> has been transmitted by the International Bureau. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US). <input checked="" type="checkbox"/> A translation of the International Application into English (35 U.S.C. 371(c)(2)). <input type="checkbox"/> A copy of the International Search Report (PCT/ISA/210). <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3)) <ol style="list-style-type: none"> <input type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau). <input type="checkbox"/> have been transmitted by the International Bureau. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired. <input checked="" type="checkbox"/> have not been made and will not be made. <input type="checkbox"/> A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)). <input type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)). <input checked="" type="checkbox"/> A copy of the International Preliminary Examination Report (PCT/IPEA/409). <input type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)). 					
Items 13 to 20 below concern document(s) or information included:					
<ol style="list-style-type: none"> <input type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98. <input type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included. <input type="checkbox"/> A FIRST preliminary amendment. <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment. <input type="checkbox"/> A substitute specification. <input type="checkbox"/> A change of power of attorney and/or address letter. <input type="checkbox"/> Certificate of Mailing by Express Mail <input checked="" type="checkbox"/> Other items or information: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> Express Mail #: EL419184179US Post Card (for stamp and return from DO/EO/US) Three (3) sheets of drawings </div> 					

Page 2 of 2

3 | PRTS

09/762649

JCO2 Rec'd PCT/PTO 09 FEB 2001

Security System

The invention relates to a security system for identity and authorization checking in a protected communication environment.

The identity and authorization checking is performed in a protected communication environment using, as a rule, personal identifiers in combination with a memory card or chip card. A user of an automatic teller machine, for instance, is required to first insert a bank card and then enter the user's personal identification number. Experience has shown that identity and authorization checks of this kind are not sufficient to avoid any abuse. It is not only awkward to enter the personal identification number, but this number is also relatively easy to spy out.

Identity and authorization checks which are considered to be very secure are those performed by means of a fingerprint sensor. High-resolution sensors operating in accordance with the principle of a capacitive matrix have been disclosed, which derive unique and unmistakable characteristics from a fingerprint and, after a highly effective data reduction, make such characteristics available as a characteristic data set. This characteristic data set may, in one application, be stored as an access and authorization condition. In such a system the entry of a personal identification code is not required. However, it can not be excluded in principle that the characteristic data set provided by the fingerprint sensor is intercepted or spied out while on its transmission path.

The invention creates a security system which provides very high protection while doing without the user having to enter a personal identification code. According to the

09762649, 040901

invention, the security system comprises a chip card reader in the format of a PC card which has personal data stored thereon. Coupled to the chip card reader is a fingerprint sensor. A validation means validates the personal information read from the chip card depending on data provided by the fingerprint sensor. For a positive outcome of an identity and authorization check, both the chip card with the personal data needs to be available and also the characteristic data set provided by the fingerprint sensor needs to be correctly related to the personal data stored on the chip card.

The security system in accordance with the invention allows to establish a highly secure control of the communication between a local data processing apparatus and a network. According to a first approach, in which the fingerprint sensor is integrated in the chip card reader, the security system comprises an interface for connection to the network. The interface involved may be a conventional network media adapter, a modem, or an IR interface. The local data processing apparatus and the network can communicate only via the security system. By providing such a security system it can be ensured that only authorized users are permitted to access the network. Provision can further be made that all messages transmitted in one or in both directions are signed by the characteristic data set provided by the fingerprint sensor and are thus authenticated.

A second approach consists in arranging the fingerprint sensor on a module coupled with the chip card reader by a detachable plug connection. In this approach, in order to prevent the characteristic data set provided by the fingerprint sensor from being spied out in the environment of the plug connection, this characteristic data set is not transmitted directly, but in an encoded form. To this end, the module is provided with a SAM card reader and an internal processor. Using such an embodiment of the security system,

09762549-040901

communication between a local data processing apparatus and a network or the like may also be controlled with a maximum degree of security.

Further features and advantages of the invention will be obvious from the following description and from the drawings to which reference is made and in which:

Figure 1 is a schematic side view of a chip card reader with a chip card inserted and the sensor module slipped on;

Figure 2 is a view of an end face of the sensor module;

Figure 3 is a top view of the sensor module, with the chip card shown cut off;

Figure 4 shows three possible embodiments for the housing of the sensor module;

Figure 5 is a schematic side view of the chip card reader and the sensor module according to a further embodiment;

Figure 6 is a view of an end face of the sensor module;

Figure 7 is a top view of the sensor module;

Figure 8 is a schematic side view of a further embodiment of the chip card reader and the sensor module; and

Figure 9 is a block diagram of the security system.

The security system, shown in Figure 1, for identity and authorization checking in a protected communication environment comprises a chip card reader 10 in the format of a PC card and a sensor module 12 which has a fingerprint sensor 14 and is detachably coupled to the chip card reader 10 by a plug connection. The chip card reader 10 includes an accommodation channel for a chip card 16 and, arranged in the accommodation channel, a contact field 18 for contacting the chip card 16. In the case of the embodiment shown here, the

09752649 040901

accommodation channel for the chip card is formed between a cover plate 10a and the main body 10b of the chip card reader.

The sensor module 12 is coupled to the narrow end face of the chip card reader 10, from which the chip card 16 projects. The housing of the sensor module 12 is provided with a slot 20 for the passage of the chip card 16. The fingerprint sensor 14 is embedded in the upper main surface of the sensor module 12. The sensor module 12 has a pair of guide pins 24 which are insertable into corresponding receiving openings at the narrow end face of the chip card reader 10. A series of contact pins 26 of the sensor module 12 are adapted to be inserted into corresponding contact ports on the same end face of the chip card reader 10. Actuating members 28 for a locking means are mounted on the narrow sides of the sensor module 12; by means of the locking means the sensor module 12 is detachably locked with the chip card reader 10. Figure 3 also illustrates the contact surface 16a of the chip card 16. With the chip card 16 inserted in the chip card reader 10, the contact surface 16a ends up lying beneath the contact field 18.

Depending on how the accommodation channel for the chip card 16 is arranged in the chip card reader, the slot 20 to be seen in Figure 2 is provided in the housing of the sensor module 12, or otherwise, recesses 20a and 20b are provided at the underside and at the upper side, respectively, of the sensor module 12, as illustrated in Figure 4.

In the embodiment illustrated in Figure 5, the sensor module 12 has formed thereon a housing block with a ramp-shaped supporting surface in which the fingerprint sensor 14 is embedded. In addition, the sensor module 12 is configured for receiving and reading a so-called SAM card or SIM card 32. The card in question is a known security and authentication module.

A further component of the sensor module 12 is an interface for the connection to a communication system; in the embodiment shown, this is a network media adapter to which a network cable 34 is connected by means of a plug connector 36.

Figure 8 shows an embodiment of the chip card reader with an accommodation channel for the chip card which is formed between a bottom plate and the main body of the chip card reader.

The concept underlying the security system will now be explained with reference to the block diagram in Figure 9.

The security system comprised of the chip card reader 10 with chip card 16, on the one hand, and the sensor module 12 with the fingerprint sensor 14 and the SAM card 32, on the other hand, is fitted between a data processing apparatus (PC) referred to as host and a network connection. The chip card reader 10, just like the sensor module 12, is provided with a separate local bus. The two bus systems are coupled with each other via the plug connection between the chip card reader 10 and the sensor module 12. The chip card reader 10 includes an internal processor 40 which assumes the functions of authentication, identification, cryptographic coding, and signature. On the host side the chip card reader 10 is equipped with a suitable interface 42, more particularly a PCMCIA interface. The chip card reader 10 further includes a storage 44 for secured data in flash technology and a time stamping unit 46 which may include a radio-controlled clock module. The chip card 16 is designed as a so-called smart card and has processor and storage circuits of its own. In particular, personal keys and code words for the purpose of identity and authorization checking are stored in the chip card 16. All of the above-mentioned components of the chip card reader 10 are coupled to its internal local bus.

The sensor module 12 likewise comprises an internal processor 50, the task of which consists, above all, in the analysis of the fingerprint data provided by the sensor 14 for the purpose of identification. The SAM card is read out via a contact unit 52. The SAM card has characteristic fingerprint data of the authorized user stored thereon. The communication interface of the sensor module 12 includes an interface controller 54 and a network media adapter 56, to which the network cable 34 is connected.

In addition to the characteristic fingerprint data of the authorized user the SAM card includes data and structures for encoding such data, which is then transferred to the chip card reader 10 in an encoded form for evaluation.

An encoded transmission of the fingerprint data can be done without if the fingerprint sensor and the chip card reader are integrated with each other, so that it is not possible to intercept the data from the fingerprint sensor. In the case of this alternative embodiment, the communication interface (network media adapter) is integrated in the system as well.

106040" 64929260

Claims

1. A security system for identity and authorization checking in a protected communication environment, comprising:

- a chip card reader in the format of a PC card;
- a chip card having personal data stored thereon;
- a fingerprint sensor which is coupled to the chip card reader;
- a validation means for validating the personal information read from the chip card depending on data provided by the fingerprint sensor.

2. The security system according to claim 1, characterized in that the fingerprint sensor is arranged on a module coupled with the chip card reader by a detachable plug connection.

3. The security system according to claim 2, characterized in that the module is adapted to be slipped onto a narrow end face of the chip card reader from which the chip card projects.

5. The security system according to claim 3, characterized in that a slot is disposed in the module for the chip card to pass therethrough.

6. The security system according to any of claims 2 to 5, characterized in that the module includes a SAM or SIM card reader.

7. The security system according to claim 6, characterized in that the data provided by the fingerprint sensor is processed along with the data read from the SAM or SIM card in an internal processor of the module to yield an encoded identity information.

106040 64929250

8. The security system according to any of claims 1 to 7, characterized by an interface for the connection to a communication system, in particular a network.

9. The security system according to claims 2 and 8, characterized in that the interface is contained in the module.

10. The security system according to claim 8 or 9, characterized in that signed messages are able to be exchanged with the communication environment via the interface.

092649 040901 06040 64929260

Abstract

A security system for identity and authorization checking in a protected communication environment is based on the use of a chip card reader in the format of a PC card. The chip card has personal data stored thereon. A fingerprint sensor is coupled to the chip card reader. The personal information read from the chip card is validated depending on data provided by the fingerprint sensor.

Figure 1

040904-0600

FIG. 1

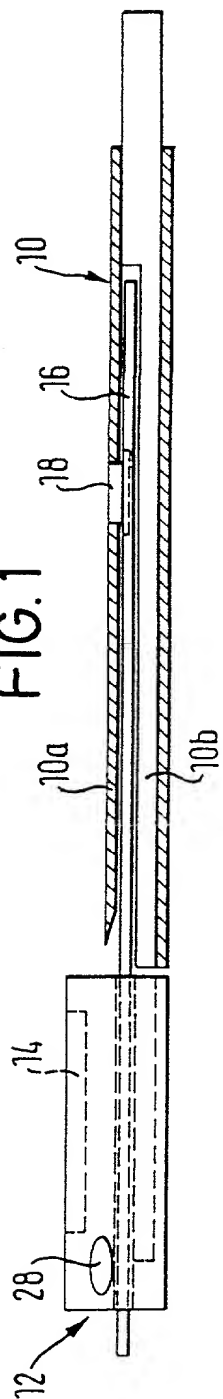


FIG. 2

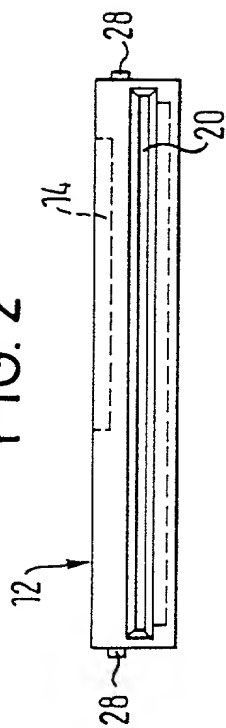


FIG. 3

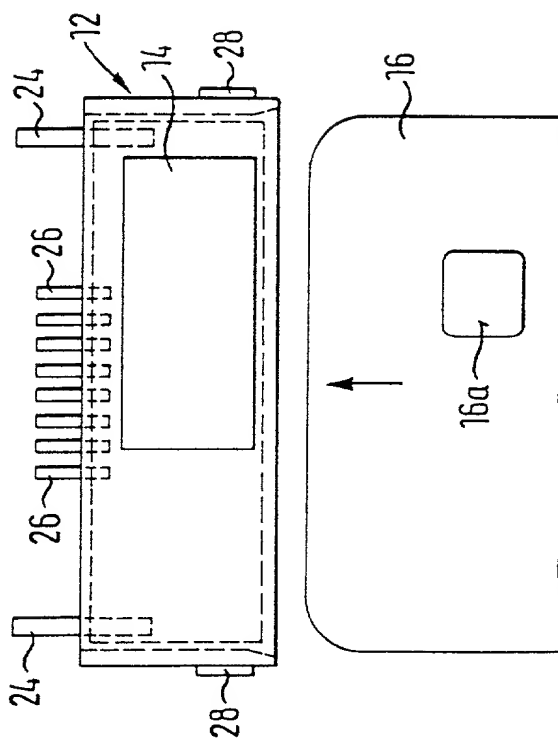
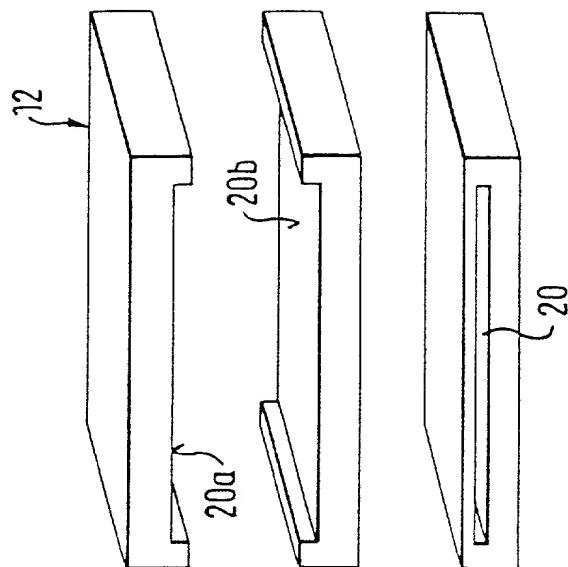
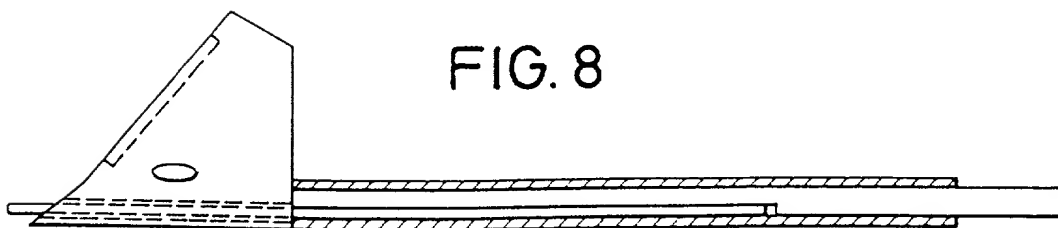
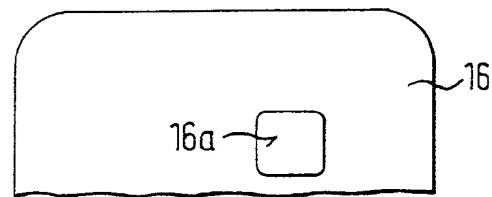
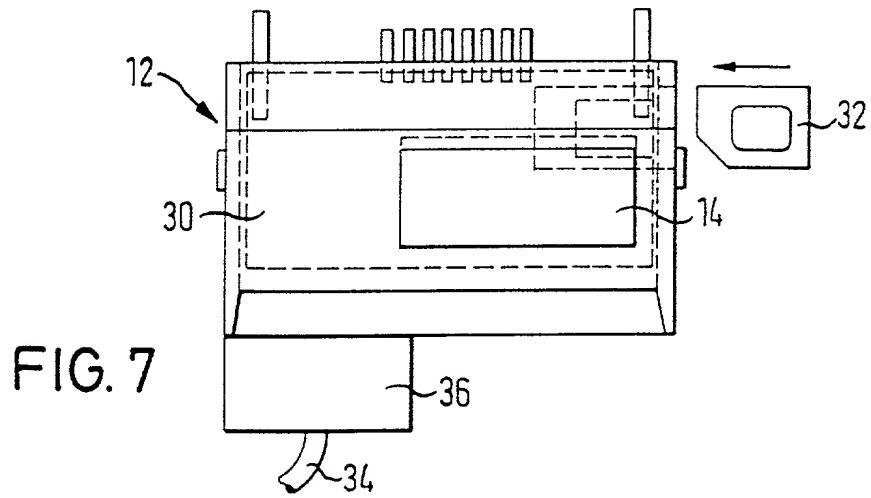
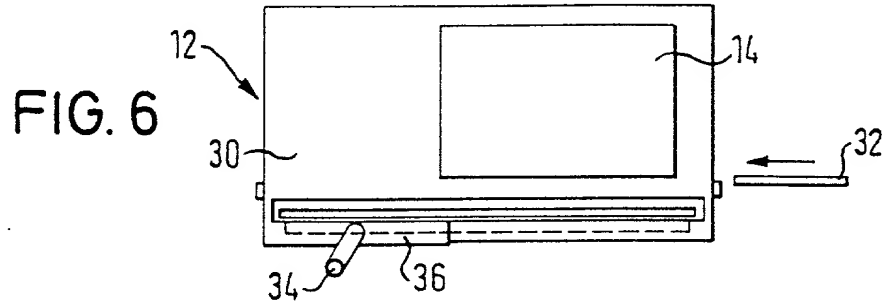
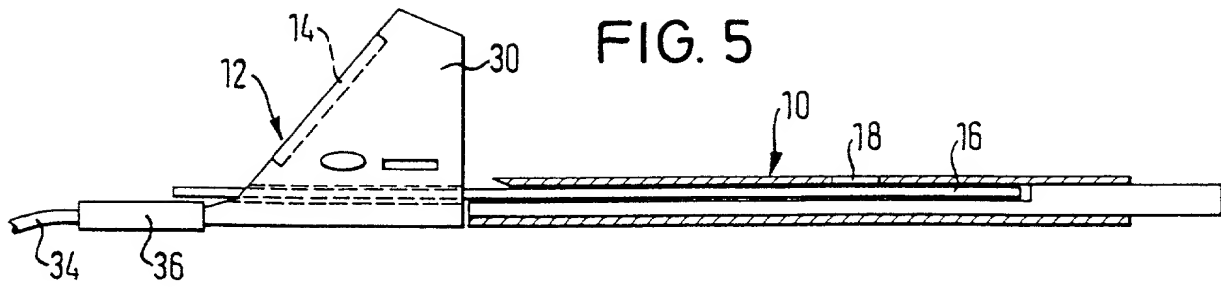
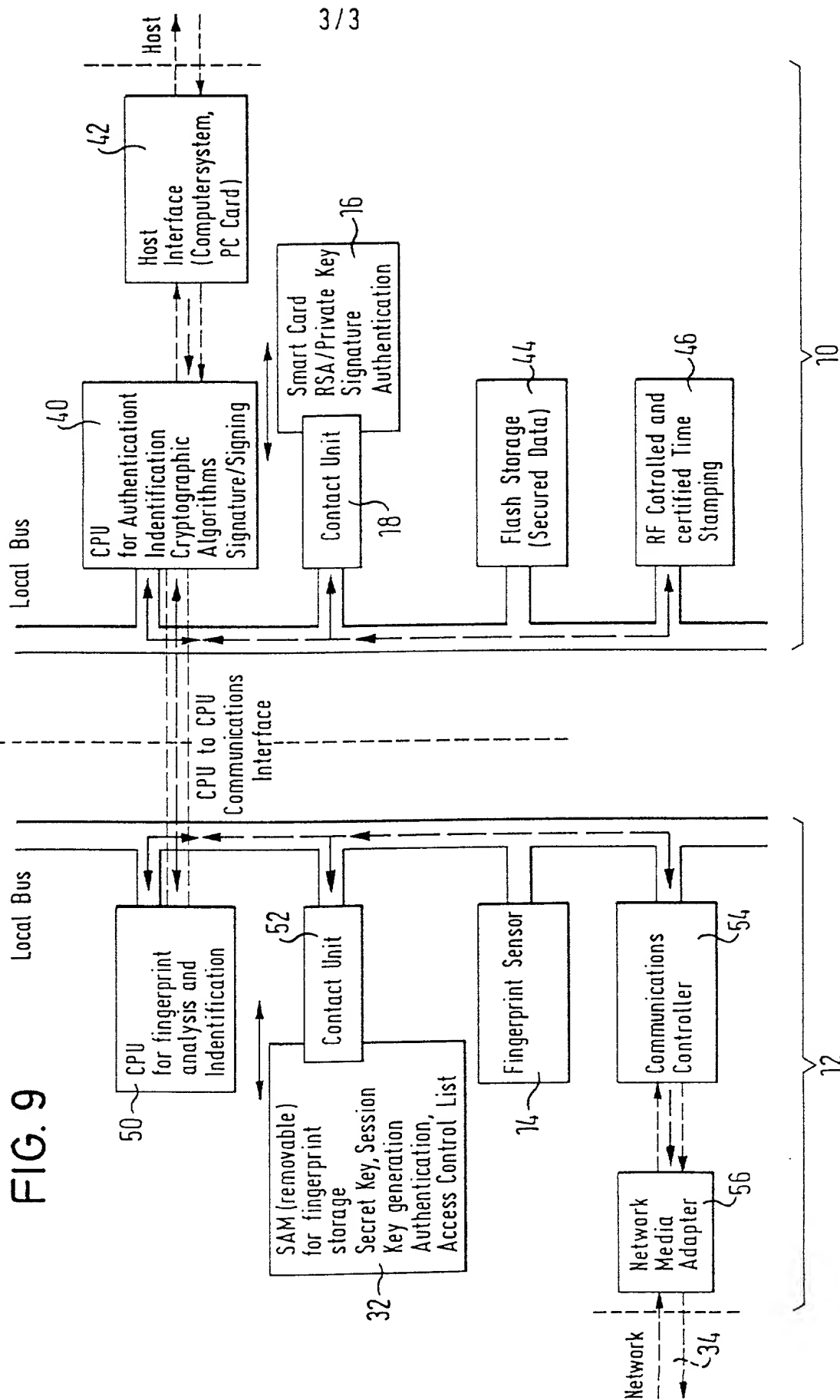


FIG. 4





Overview on Security System
Detachable Fingerprint Module Detachable PC Card Smart Card Reader



Docket No.
6761-60186

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

SECURITY SYSTEM

the specification of which

(check one)

☐ is attached hereto.

☒ was filed on February 9, 2001 as United States Application No. or PCT International

Application Number 09/762,649

and was amended on _____

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Not Claimed

298 14 427.1

Germany

11 August 1998

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional

(Application Serial No.)

(Filing Date)

(Application Serial No.)

(Filing Date)

(Application Serial No.)

(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

PCT/EP99/05879
(Application Serial No.)

11 August 1999
(Filing Date)

National Phase (abandoned)
(Status)
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Martin F. Majestic	Reg. No. 25,695
J. Bruce McCubrey	Reg. No. 20,687
Donald L. Bartels	Reg. No. 28,282
David Schnapf	Reg. No. 31,566
Robert D. Becker	Reg. No. 37,778
James W. Drapinski	Reg. No. 46,242
John W. Carpenter	Reg. No. 26,447
Hal R. Yeager	Reg. No. 35,419
Tom Brody	Reg. No. 46,443
Keiichi Nishimura	Reg. No. 29,093
Steyen R. Vosen	Reg. No. 45,186

Send Correspondence to: Martin F. Majestic
COUDERT BROTHERS
 Four Embarcadero Center, Suite 3300
 San Francisco, California 94111

Direct Telephone Calls to: (name and telephone number)
 Martin F. Majestic, (415) 986-1300

Full name of sole or first inventor

Wolfgang Neifer

Sole or first inventor's signature

Residence

Altenhauserstrasse 13, 85356 Freising, GERMANY

Citizenship

Post Office Address

Date

03/30/01

Full name of second inventor, if any

Second inventor's signature

Date

Residence

Citizenship

Post Office Address